Docket No. 249943US6

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Masahiro SUEYOSHI, et al. GAU:

SERIAL NO: NEW APPLICATION EXAMINER:

FILED: HEREWITH

FOR: DATA PROCESSING DEVICE AND METHOD AND PROGRAM OF SAME

REQUEST FOR PRIORITY

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

☐ Full benefit of the filing date of U.S. Application Serial Number , filed , is claimed pursuant to the provisions of **35 U.S.C. §120**.

☐ Full benefit of the filing date(s) of U.S. Provisional Application(s) is claimed pursuant to the provisions of **35 U.S.C. §119(e)**: **Application No.** **Date Filed**

■ Applicants claim any right to priority from any earlier filed applications to which they may be entitled pursuant to the provisions of **35 U.S.C. §119**, as noted below.

In the matter of the above-identified application for patent, notice is hereby given that the applicants claim as priority:

COUNTRY	APPLICATION NUMBER	MONTH/DAY/YEAR
Japan	2003-070301	March 14, 2003

Certified copies of the corresponding Convention Application(s)

■ are submitted herewith

☐ will be submitted prior to payment of the Final Fee

☐ were filed in prior application Serial No. filed

☐ were submitted to the International Bureau in PCT Application Number
Receipt of the certified copies by the International Bureau in a timely manner under PCT Rule 17.1(a) has been acknowledged as evidenced by the attached PCT/IB/304.

☐ (A) Application Serial No.(s) were filed in prior application Serial No. filed ; and

☐ (B) Application Serial No.(s)

- ☐ are submitted herewith
- ☐ will be submitted prior to payment of the Final Fee

Respectfully Submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Bradley D. Lytle
Registration No. 40,073

C. Irvin McClelland
Registration Number 21,124

Customer Number
22850
Tel. (703) 413-3000
Fax. (703) 413-2220
(OSMMN 05/03)

S04P0337US00

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月１４日

出願番号
Application Number: 特願２００３－０７０３０１

[ST. 10/C]: ［ＪＰ２００３－０７０３０１］

出願人
Applicant(s): ソニー株式会社

２００３年１２月１０日

特許庁長官
Commissioner,
Japan Patent Office 今井康夫

出証番号　出証特２００３－３１０２３５９

【書類名】　特許願
【整理番号】　0390086803
【提出日】　平成15年 3月14日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 7/00
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　末吉　正弘
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　舘野　啓
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　平野　義昭
【発明者】
【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
【氏名】　照山　勝幸
【特許出願人】
【識別番号】　000002185
【氏名又は名称】　ソニー株式会社
【代理人】
【識別番号】　100094053
【弁理士】
【氏名又は名称】　佐藤　隆久

【手数料の表示】

【予納台帳番号】　014890

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707389

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ処理装置、その方法およびそのプログラム

【特許請求の範囲】

【請求項１】

鍵データを基に認証先との間で認証を行う認証手段と、

前記認証手段から受けたデータを基に前記鍵データを生成して前記認証手段に提供する鍵生成手段と

を有し、

前記認証手段は、第１のデータと第２のデータとを前記鍵生成手段に提供し、

前記鍵生成手段は、前記認証手段から受けた前記第１のデータと前記第２のデータとのうち前記第１のデータのみを用いて前記鍵データを生成する

データ処理装置。

【請求項２】

前記鍵生成手段は、前記認証手段から受けたデータを基に、当該認証先に固有の前記鍵データを生成する

請求項１に記載のデータ処理装置。

【請求項３】

前記鍵生成手段は、第１の入力パラメータおよび第２の入力パラメータを持ち、前記第１の入力パラメータに代入された前記第１のデータのみを用いて前記鍵データを生成する機能モジュールを備え、

前記認証手段は、前記鍵生成手段の前記機能モジュールの前記第１の入力パラメータに前記第１のデータを代入し、前記第２の入力パラメータに前記第２のデータを代入する

請求項１に記載のデータ処理装置。

【請求項４】

前記認証手段は、前記認証の後に行う処理に関する識別データであり前記認証先から受けた前記第１のデータおよび前記第２のデータを前記鍵生成手段に提供する

請求項１に記載のデータ処理装置。

【請求項５】

前記認証手段は、前記認証先から受けた当該認証先に固有の固有データを提供する処理を行う機能モジュールを備え、

前記鍵生成手段は、前記認証手段の前記機能モジュールを呼び出し、当該機能モジュールから受けた前記固有データをさらに用いて、前記鍵データを生成する

請求項１に記載のデータ処理装置。

【請求項６】

前記認証手段は、前記機能モジュールを規定する関数を含む認証プログラムを実行手段で実行して実現され、

前記鍵生成手段は、前記機能モジュールの呼び出し手順を含む鍵生成プログラムを前記実行手段で実行して実現される

請求項５に記載のデータ処理装置。

【請求項７】

前記認証手段は、前記鍵生成手段によって前記機能モジュールが呼び出されると、当該機能モジュールの実行に応じて、前記認証手段と前記鍵生成手段とで共用される記憶手段から読み出した前記固有データを前記鍵生成手段に提供する

請求項５に記載のデータ処理装置。

【請求項８】

マスタ鍵データを読み出す機能モジュールを備え、前記マスタ鍵データを保持する鍵保持手段

をさらに有し、

前記鍵生成手段は、前記鍵保持手段の前記機能モジュールを呼び出し、当該機能モジュールが取り出した前記マスタ鍵データをさらに用いて前記鍵データを生成する

請求項１に記載のデータ処理装置。

【請求項９】

前記鍵保持手段は、鍵保持プログラムを実行手段で実行して実現される

請求項８に記載のデータ処理装置。

【請求項１０】

前記鍵保持プログラムは、前記認証手段および前記鍵生成手段を実現するプログラムとは独立して更新される

請求項９に記載のデータ処理装置。

【請求項１１】

前記鍵生成手段は、前記認証の後に行われる複数の処理内容のそれぞれに対応して規定された異なる複数の鍵生成アルゴリズムのうち、指定された処理内容に対応した前記鍵生成アルゴリズムを選択し、当該選択した鍵生成アルゴリズムを基に、当該認証先に固有の前記鍵データを生成する

請求項１に記載のデータ処理装置。

【請求項１２】

前記認証手段は、前記鍵データを基に前記認証先との間の認証を行い、前記認証先との間で互いの正当性を認めると、前記鍵データに対応付けられた処理を前記認証先と連携して行う

請求項１に記載のデータ処理装置。

【請求項１３】

前記鍵生成手段は、前記認証先に固有の前記第１のデータを基に当該認証先に固有の個別鍵データを生成し、

前記認証手段は、当該認証手段が保持する複数の前記認証先で共用される固定鍵データを用いて前記認証先との間で第１の認証を行い、前記鍵生成手段が生成した前記個別鍵データを用いて前記認証先との間で第２の認証を行う

請求項１に記載のデータ処理装置。

【請求項１４】

前記認証手段は、前記第１の認証により前記認証先の正当性を確認した後に前記認証先と連携して前記固定鍵データに対応付けられた第１の処理を行い、前記第２の認証により前記認証先の正当性を確認した後に前記認証先と連携して前記個別鍵データに対応付けられた第２の処理を行う

請求項１３に記載のデータ処理装置。

【請求項１５】

前記認証手段は、前記第２の認証に関連付けられた原鍵データを保持し、

前記鍵生成手段は、前記認証手段を介して前記認証先から受けた固有データと前記認証手段が保持する前記原鍵データとを基に、前記個別鍵データを生成する

請求項１３に記載のデータ処理装置。

【請求項１６】

前記認証手段は、前記認証先との間で行われる処理の識別データを、前記原鍵データと対応付けて保持し、指定された処理の前記識別データに対応付けられた前記原鍵データを前記鍵生成手段に提供し、

前記鍵生成手段は、前記認証手段が受けた前記原鍵データを基に前記個別鍵データを生成する

請求項１５に記載のデータ処理装置。

【請求項１７】

鍵生成手段が生成した鍵データを基に認証手段が認証先との間で認証を行うデータ処理方法であって、

前記認証手段が、前記鍵生成手段に第１のデータと第２のデータとを提供する第１の工程と、

前記鍵生成手段が、前記第１の工程で得た前記第１のデータおよび前記第２のデータのうち前記第１のデータのみを用いて鍵データを生成し、当該鍵データを前記認証手段に提供する第２の工程と、

前記認証手段が、前記第２の工程で受けた前記鍵データを基に認証先と認証を行う第３の工程と

を有するデータ処理方法。

【請求項１８】

前記第２の工程において、前記鍵生成手段が、前記第１の工程で前記認証手段から受けたデータを基に、当該認証先に固有の前記鍵データを生成する

請求項１７に記載のデータ処理方法。

【請求項１９】

前記第２の工程において、前記鍵生成手段が、第１の入力パラメータおよび第２の入力パラメータを持つ機能モジュールを基に、当該機能モジュールの前記第１の入力パラメータに代入された前記第１のデータのみを用いて前記鍵データを

生成し、

前記第１の工程において、前記認証手段が、前記鍵生成手段の前記機能モジュールの前記第１の入力パラメータに前記第１のデータを代入し、前記第２の入力パラメータに前記第２のデータを代入する

請求項１７に記載のデータ処理方法。

【請求項２０】

前記第２の工程において、前記鍵生成手段が、前記認証手段の機能モジュールを呼び出し、当該機能モジュールを基に得た前記認証先に固有の固有データをさらに用いて前記鍵データを生成する

請求項１７に記載のデータ処理方法。

【請求項２１】

前記第２の工程において、前記鍵生成手段が、鍵保持手段の機能モジュールを呼び出し、当該機能モジュールから得られた前記鍵保持手段が保持する前記マスタ鍵データをさらに用いて前記鍵データを生成する

請求項１７に記載のデータ処理方法。

【請求項２２】

前記鍵保持手段を実現する鍵保持プログラムを、前記認証手段および前記鍵生成手段を実現するプログラムとは独立して更新する第４の工程

をさらに有する請求項２１に記載のデータ処理方法。

【請求項２３】

鍵データを基に認証先と認証を行う手順を記述した認証プログラムに対して前記鍵データを提供する手順を記述し、データ処理装置で実行されるプログラムであって、

前記認証プログラムから第１のデータと第２のデータとを受ける第１の手順と、

前記第１の手順で受けた前記第１のデータと前記第２のデータとのうち前記第１のデータのみを用いて前記鍵データを生成する第２の手順と、

前記第２の手順で生成した前記鍵データを前記認証プログラムに提供する第３の手順と

の記述を有するプログラム。

【請求項２４】

前記第２の手順は、前記第１の手順で受けた前記第１のデータを基に、当該認証先に固有の前記鍵データを生成する

請求項２３に記載のプログラム。

【請求項２５】

第１の入力パラメータおよび第２の入力パラメータを持ち、前記第１の入力パラメータに代入された前記第１のデータのみを用いて前記鍵データを生成する手順を示す関数

をさらに有し、

前記第１の手順は、前記関数の前記第１の入力パラメータおよび前記第２の入力パラメータを介してそれぞれ前記第１のデータおよび前記第２のデータを受け、

前記第２の手順は、前記関数の前記第１の入力パラメータを介して受けた前記第１のデータのみを用いて前記鍵データを生成する

請求項２３に記載のプログラム。

【請求項２６】

前記認証プログラムとは異なるアクセス権限が規定されている

請求項２３に記載のプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、認証先との間で鍵データを用いた認証を行うデータ処理装置、その方法およびプログラムに関する。

【０００２】

【従来の技術】

例えば、鍵データを基に認証先と認証を行い、認証により相手の正当性を確認した後に種々の処理を行うデータ処理装置がある。

このようなデータ処理装置には、例えば、鍵データを基にした認証を行う認証

機能と、上記鍵データを生成する鍵生成機能とがある。

従来のデータ処理装置は、上記認証機能と鍵生成機能とが混在して構成されている。

【０００３】

【発明が解決しようとする課題】

上述した従来のデータ処理装置では、認証機能と鍵生成機能とを異なる開発者が開発させ、鍵生成機能が使用する鍵生成アルゴリズムを、認証機能の開発者に対して秘密にしたいという要請がある。

しかしながら、上述した従来のデータ処理装置では、認証機能と鍵生成機能とが混在しているため、上述した要請に応えることが困難であるという問題がある。

【０００４】

本発明はかかる事情に鑑みてなされたものであり、その目的は、鍵生成手段における鍵データの生成手法を認証手段の開発者に秘密にできるデータ処理装置、その方法およびそのプログラムを提供することを目的とする。

【０００５】

【課題を解決するための手段】

上記の目的を達成するため、第１の発明のデータ処理装置は、鍵データを基に認証先との間で認証を行う認証手段と、前記認証手段から受けたデータを基に前記鍵データを生成して前記認証手段に提供する鍵生成手段とを有し、前記認証手段は、第１のデータと第２のデータとを前記鍵生成手段に提供し、前記鍵生成手段は、前記認証手段から受けた前記第１のデータと前記第２のデータとのうち前記第１のデータのみを用いて前記鍵データを生成する。

【０００６】

第１の発明のデータ処理装置の作用は以下のようになる。

認証手段が、第１のデータと第２のデータとを前記鍵生成手段に提供する。

そして、鍵生成手段が、前記認証手段から受けた前記第１のデータと前記第２のデータとのうち前記第１のデータのみを用いて前記鍵データを生成する。

そして、認証手段が、前記鍵生成手段が生成した前記鍵データを基に認証先と

認証を行う。

【０００７】

また、第１の発明のデータ処理装置は、好ましくは、前記鍵生成手段は、前記認証手段から受けたデータを基に、当該認証先に固有の前記鍵データを生成する。

また、第１の発明のデータ処理装置は、好ましくは、前記鍵生成手段は、第１の入力パラメータおよび第２の入力パラメータを持ち、前記第１の入力パラメータに代入された前記第１のデータのみを用いて前記鍵データを生成する機能モジュールを備え、前記認証手段は、前記鍵生成手段の前記機能モジュールの前記第１の入力パラメータに前記第１のデータを代入し、前記第２の入力パラメータに前記第２のデータを代入する。

【０００８】

第２の発明のデータ処理方法は、鍵生成手段が生成した鍵データを基に認証手段が認証先との間で認証を行うデータ処理方法であって、前記認証手段が、前記鍵生成手段に第１のデータと第２のデータとを提供する第１の工程と、前記鍵生成手段が、前記第１の工程で得た前記第１のデータおよび前記第２のデータのうち前記第１のデータのみを用いて鍵データを生成し、当該鍵データを前記認証手段に提供する第２の工程と、前記認証手段が、前記第２の工程で受けた前記鍵データを基に認証先と認証を行う第３の工程とを有する。

【０００９】

第３の発明のプログラムは、鍵データを基に認証先と認証を行う手順を記述した認証プログラムに対して前記鍵データを提供する手順を記述し、データ処理装置で実行されるプログラムであって、前記認証プログラムから第１のデータと第２のデータとを受ける第１の手順と、前記第１の手順で受けた前記第１のデータと前記第２のデータとのうち前記第１のデータのみを用いて前記鍵データを生成する第２の手順と、前記第２の手順で生成した前記鍵データを前記認証プログラムに提供する第３の手順との記述を有する。

【００１０】

【発明の実施の形態】

以下、本発明の実施形態に係わるカードシステムについて説明する。

図１は、本実施形態のカードシステム１の構成図である。

図１に示すように、カードシステム１は、例えば、Ｒ／Ｗ(Reader/Writer) １１を介してＩＣカード１０のＩＣ(Integrated Circuit)１５とＳＡＭ(Secure Application Module) １２とが認証を行った後に、連携して所定のサービスに関する処理を行う。

ここで、ＳＡＭ１２が本発明のデータ処理装置に対応し、ＩＣ１５が本発明の認証先に対応している。

また、管理装置１３は、ＳＡＭ１２とＩＣ１５の間の相互認証に用いられる鍵データ等を格納した鍵パッケージＫＰをＳＡＭ１２に登録する。

また、ＳＡＭ１２の管理者、例えば、ＩＣカード１０を利用した所定のサービスの提供者は、複数のユーザの各々にＩＣカード１０を発行する。

【００１１】

ＩＣ１５は、後述するように、ＳＡＭ１２を利用してＩＣ１５のユーザが受ける種々のサービスに関するデータおよびプログラムのファイルデータを記憶しており、当該ファイルデータを用いたサービスに利用権限が設定されている。具体的には、ＩＣ１５とＳＡＭ１２とが指定されたサービスに対応付けられた鍵データを基に相互認証を行い、お互いの正当性を確認したことを条件に、ＩＣ１５とＳＡＭ１２とが連携して上記サービスに係わる処理を行う。

本実施形態では、上記複数のユーザの各々に発行されたＩＣカード１０には、上記認証に用いられる鍵データの一部として、個々のＩＣカード１０に固有の鍵データ（本発明の鍵データまたは個別鍵データ）が割り当てられている。

そして、ＳＡＭ１２は、ＩＣカード１０から、当該ＩＣカード１０の固有データ、例えば、製造時にＩＣカード１０に固有に割り当てられたシリアル番号などの装置識別データＩＤＭと、指定されたサービス等を識別する複数の識別データＳＩＤ１，ＳＩＤ２、ＳＩＤ３とを入力し、これらを基に所定のアルゴリズムで認証に用いる上記鍵データを生成する。

【００１２】

以下、図１に示す各構成要素について説明する。

〔ＩＣ１５〕

図２は、図１に示すＩＣカード１０に内蔵されたＩＣ１５の構成図である。

図２に示すように、ＩＣ１５は、例えば、インタフェース２１、メモリ２２およびＣＰＵ２３を有し、これらが内部バス２０を介して接続されている。

インタフェース２１は、Ｒ／Ｗ１１を介してＳＡＭ１２との間でデータの授受を行う。

メモリ２２は、ＳＡＭ１２を利用してＩＣ１５のユーザが受ける種々のサービスに関する処理に用いられるデータおよびプログラムのファイルデータを記憶している。

また、メモリ２２は、上記サービスに関する処理を行う前にＳＡＭ１２との間の認証に用いられる種々の鍵データを記憶している。

また、メモリ２２は、個々のＩＣカード１０に固有の装置識別データＩＤＭを記憶している。

【００１３】

なお、ＳＡＭ１２は、例えば、同じ機種のＳＡＭ１２に共通して割り当てられたシステムコードに対応付けられた鍵データを基に相互認証を行い、当該相互認証により互いの正当性が認められたことを条件に、ＩＣ１５に対してのアクセスが許可される。

さらに、メモリ２２内で種々のサービスのファイルデータは、それぞれ階層構造を有するフォルダであるエリア内に格納されている。

ＳＡＭ１２は、メモリ２２内のエリアのエリアコードに対応付けられた鍵データを基に相互認証を行い、当該相互認証により互いの正当性が認められたことを条件に、当該エリアに対してのアクセスが許可される。

さらに、ＳＡＭ１２は、エリア内に記憶されたファイルデータのサービスコードに対応付けられた鍵データを基に相互認証を行い、当該相互認証により互いの正当性が認められたことを条件に、当該ファイルデータに対してのアクセスが許可される。

【００１４】

本実施形態では、図３に示すように、ＩＣ１５に関して上述したように規定さ

れた鍵データの種類には、固定鍵データと個別鍵データとが規定されている。

固定鍵データは、例えば、複数のＩＣカード１０のＩＣ１５の間で、ファイルシステム上の位置が同一であれば、その値が同じである鍵データである。すなわち、固定鍵データは、複数のＩＣカード１０のＩＣ１５で共用される鍵データである。

個別鍵データは、複数のＩＣカード１０のＩＣ１５の間で、ファイルシステム上の位置が同一であっても、その値が異なる鍵データである。すなわち、個別鍵データは、複数のＩＣカード１０のＩＣ１５の各々で固有の鍵データである。

なお、ＩＣ１５は、上記鍵データが固定鍵データおよび個別鍵データのいずれであるかを特定することなく処理を行う。

【００１５】

ＣＰＵ２３は、メモリ２２から読み出したプログラム、並びに鍵データを基に、インタフェース２１およびＲ／Ｗ１１を介して、ＳＡＭ１２とデータの授受を行ってＳＡＭ１２と相互認証を行う。

また、ＣＰＵ２３は、上記相互認証で互いの正当性を確認すると、ＳＡＭ１２と連携して、相互認証で用いた鍵データに対応付けられたサービスに関する処理を実行する。

また、ＣＰＵ２３は、例えば、ＩＣカード１０の発行時に、所定の権限が認証された管理者の操作に応じて、インタフェース２１を介して暗号化された鍵パッケージを復号し、当該復号した鍵パッケージ内の上記鍵データをメモリ２２に書き込む。

【００１６】

〔ＳＡＭ１２〕

図４は図１に示すＳＡＭ１２の機能ブロック図、図５は認証時におけるＳＡＭ１２のデータの流れを説明するための図、図６はＳＡＭ１２のソフトウェア構成を説明するための図である。

図４に示すように、ＳＡＭ１２は、例えば、インタフェース３１、カード処理部３２、鍵管理部３３、鍵生成部３４および鍵保存部３５を有し、これらが内部バス３０を介して接続されている。

本実施形態において、カード処理部３２および鍵管理部３３が本発明の認証手段に対応し、鍵生成部３４が本発明の鍵生成手段に対応し、鍵保存部３５が本発明の鍵保持手段に対応している。

【００１７】

また、図６に示すように、カード処理部３２および鍵管理部３３は、認証プログラム８０（本発明の認証プログラム）をＣＰＵ（図示しない）などのデータ処理装置（本発明の実行手段またはデータ処理装置）で実行して実現される。

また、鍵生成部３４は、鍵生成プログラム８１（本発明のプログラムまたは鍵生成プログラム）を上記ＣＰＵなどのデータ処理装置で実行して実現される。

また、鍵保存部３５は、鍵保存プログラム８２（本発明の鍵保存プログラム）を上記ＣＰＵなどのデータ処理装置で実行して実現される。

【００１８】

本実施形態では、図７に示すように、認証プログラム８０にファイアウォールＦＷ１が規定され、鍵生成プログラム８１および鍵保存プログラム８２にファイアウォールＦＷ２が規定されている。

すなわち、ファイアウォールＦＷ１，ＦＷ２により、鍵生成プログラム８１および鍵保存プログラム８２へのアクセス権限は、認証プログラム８０へのアクセス権限とは別に規定されている。

具体的には、ＳＡＭ１２内において、鍵生成プログラム８１および鍵保存プログラム８２が記憶された記憶領域へのアクセス権限は、認証プログラム８０が記憶された記憶領域へのアクセス権限とは別に規定されている。

従って、認証プログラム８０へのアクセス権限を有する者でも、認証プログラム８０および鍵生成プログラム８１へのアクセス権限を有しない場合には、認証プログラム８０および鍵生成プログラム８１へのアクセスは禁止される。

また、鍵保存プログラム８２は、鍵生成プログラム８１および認証プログラム８０のダウンロードとは独立して、ＳＡＭ１２の外部からダウンロードされる。

【００１９】

また、本実施形態では、認証プログラム８０から鍵生成プログラム８１に、ＩＣ１５の装置識別データＩＤＭと、サービス等の複数の識別データＳＩＤ１，Ｓ

ＩＤ２，ＳＩＤ３を提供する。

そして、鍵生成プログラム８１は、認証プログラム８０から入力した上記データのうち、装置識別データＩＤＭと識別データＳＩＤ２（本発明の第１のデータ）とを基に、個別鍵データＫＩ（本発明の鍵データ）を生成する。すなわち、鍵生成プログラム８１は、認証プログラム８０から入力した識別データＳＩＤ１，ＳＩＤ３（本発明の第２のデータ）を、個別鍵データＫＩの生成に用いない。

【００２０】

以下、鍵生成プログラム８１と、認証プログラム８０および鍵保存プログラム８２との間でのデータの授受の手法を説明する。

本実施形態では、図６に示すように、認証プログラム８０は、鍵生成プログラム８１内のＡＰＩ(Application Program Interface) 関数である関数ＡＰＩ１を呼び出し、下記式（１）に示すように、当該関数ＡＰＩ１の入力パラメータとして、ＩＣカードのＩＣ５から入力したサービス等の識別データＳＩＤ１，２，３を代入する記述（コード）を有する。

【００２１】

【数１】

ＡＰＩ１（ＳＩＤ１，ＳＩＤ２，ＳＩＤ３）　　…（１）

【００２２】

そして、認証プログラム８０を基にした当該コードの実行に応じて、識別データＳＩＤ１，２，３が、指定されたバッファ（図示せず）内のアドレスに書き込まれる。そして、鍵生成プログラム８１内の関数ＡＰＩ１の実行に応じて、上記アドレスに書き込まれた識別データＳＩＤ１，２，３を入力パラメータとして用いて鍵生成が行われる。なお、鍵生成プログラム８１は、上記ＡＰＩ関数の実行の戻り値として受けた上記バッファ内のアドレスに、識別データＳＩＤ１，２，３を書き込んでもよい。

なお、認証プログラム８０から鍵生成プログラム８１への原鍵データＫＯの提供も、上記ＡＰＩ１関数を介して行われる。

上述したように、ＳＡＭ１２は、鍵生成プログラム８１で規定されたＡＰＩ１関数を介して、認証プログラム８０から鍵生成プログラム８１に、識別データＳ

ＩＤ１～ＳＩＤ３および原鍵データＫＯを提供する。

【００２３】

また、認証プログラム８０は、関数ＡＰＩ２を有し、ＩＣカードのＩＣ５から入力した装置識別データＩＤＭを関数ＡＰＩ２の戻り値として規定されたバッファ内のアドレスに格納する。

そして、鍵生成プログラム８１が、関数ＡＰＩ２を呼び出し、その戻り値として規定されたアドレスから、装置識別データＩＤＭを読み出す。

上述したように、ＳＡＭ１２は、認証プログラム８０で規定された関数ＡＰＩ２を介して、認証プログラム８０から鍵生成プログラム８１に装置識別データＩＤＭを提供する。

【００２４】

また、鍵保存プログラム８２は、関数ＡＰＩ３を有し、鍵保存プログラム８２が保持するマスタ鍵データＫＭを、関数ＡＰＩ３の戻り値として規定されたバッファ内のアドレスに格納する。

そして、鍵生成プログラム８１が、関数ＡＰＩ３を呼び出し、その戻り値として規定されたアドレスから、マスタ鍵データＫＭを読み出す。

上述したように、ＳＡＭ１２は、鍵保存プログラム８２で規定された関数ＡＰＩ３を介して、鍵保存プログラム８２から鍵生成プログラム８１にマスタ鍵データＫＭを提供する。

【００２５】

なお、関数ＡＰＩ１，ＡＰＩ２，ＡＰＩ３が本発明の機能モジュールに対応している。

【００２６】

以下、ＳＡＭ１２の構成要素について説明する。

インタフェース３１は、図１に示すＲ／Ｗ１１を介してＩＣ１５との間でデータ授受を行う。

カード処理部３２は、鍵管理部３３から入力した鍵データを基に、インタフェース３１を介してＩＣカード１０のＩＣ１５と相互認証を行い、当該相互認証により互いの正当性を確認すると、指定されたサービスに関する処理をＩＣ１５と

連携して行う。カード処理部３２は、アプリケーションプログラムを実行することで種々の機能を実現する。

カード処理部３２は、鍵管理部３３から入力した鍵データを基にＩＣ１５との間で相互認証を行う。

【００２７】

鍵管理部３３は、上記相互認証等に用いる鍵データを管理する鍵管理データＫＭＤを保持している。

鍵管理データＫＭＤは、図５に示すように、識別データＳＩＤと、鍵データＫと、鍵特性データＫＰＤとを対応付けて示している。

識別データＳＩＤは、ＳＡＭ１２がＩＣ１５と連携して行うサービス（ファイルデータ）および当該サービスに伴ってＩＣ１５にアクセスする記憶領域（フォルダ）等を識別するデータである。識別データＳＩＤは、例えば、ＩＣ１５から入力したシステムコード、エリアコードあるいはサービスコードである。

本実施形態では、図６に示すように、認証プログラム８０が、ＩＣカードのＩＣ５から入力した装置識別データＩＤＭと、サービス等の識別データＳＩＤ１，２，３を鍵生成プログラム８１に提供する。

【００２８】

鍵データＫは、上記サービスに先立って行うＩＣ１５との間の相互認証に用いる鍵データである。なお、個別鍵データを基に行われる処理の識別データＳＩＤには、鍵データＫとして前述した原鍵データＫＯが関連付けられている。

鍵特性データＫＰＤは、鍵データＫが前述した固定鍵データおよび個別鍵データの何れであるかを示すデータである。

【００２９】

鍵管理部３３は、鍵管理データＫＭＤの鍵特性データＫＰＤを基に、カード処理部３２からの鍵要求ＫＲＥＱ内の識別データＳＩＤが固定鍵データに対応付けられている場合には、鍵管理データＫＭＤから当該識別データＳＩＤに対応する鍵データ（固定鍵データ）Ｋを読み出してカード処理部３２に出力する。

一方、鍵管理部３３は、鍵管理データＫＭＤの鍵特性データＫＰＤを基に、カード処理部３２からの鍵要求ＫＲＥＱ内の識別データＳＩＤが個別鍵データに対

応付けられている場合には、カード処理部３２に装置識別データＩＤＭを要求し（図５中の要求ＩＤＭ＿ＲＥＱ）、それに応じて入力した装置識別データＩＤＭと、識別データＳＩＤと、鍵管理データＫＭＤから取り出した当該識別データＳＩＤに対応する鍵データＫ（図５原中の鍵データＫＯ）とを鍵生成部３４に出力する。当該識別データＳＩＤおよび原鍵データＫＯは、前述したように、関数ＡＰＩ１を介して、認証プログラム８０から鍵生成プログラム８１に提供される。

【００３０】

鍵管理部３３への鍵管理データＫＭＤの設定は、例えば、以下のように行われる。

すなわち、図１に示す管理装置１３が、図８に示すように、鍵管理データＫＭＤを設定用マスタ鍵データＫＰＭで暗号化した鍵パッケージデータＫＰを生成し、これをＳＡＭ１２に出力する。

ＳＡＭ１２は、インタフェース３１を介して入力した鍵パッケージデータＫＰを、図４に示す鍵管理部３３あるいは図示しない復号部において、設定用マスタ鍵データＫＰＭを用いて復号して鍵管理データＫＭＤを生成し、これを保持する。

ここで、鍵管理部３３への鍵管理データＫＭＤの設定をＳＡＭ１２を用いたサービスを提供する事業者が行うようにすることで、当該事業者が鍵管理をセキュアな状態で、しかも高い自由度で行うことができる。

なお、鍵管理データＫＭＤ内に格納された個別鍵の生成原となる鍵データＫＯは、個別鍵データＫＩそのものではないので、鍵管理データＫＭＤの秘匿性が失われた場合でも、個別鍵データＫＩ自体の秘匿性は失われない。

【００３１】

鍵生成部３４は、鍵保存部３５からのマスタ鍵データＫＭと、鍵管理部３３から入力した装置識別データＩＤＭと、識別データＳＩＤと、鍵データＫ（ＫＯ）とを基に、個別鍵生成プログラムＫＰＲＧを実行して鍵データ（個別鍵データ）ＫＩを生成し、これを鍵管理部３３に出力する。

鍵管理部３３は、鍵生成部３４から入力した鍵データＫＩをカード処理部３２に出力する。

鍵生成部３４は、例えば、図９に示す手順で鍵データＫＩを生成する。

図９に示す各手順は、個別鍵生成プログラムＫＰＲＧに記述されている。

以下、図９に示す各ステップを説明する。

ステップＳＴ１１：

鍵生成部３４は、前述したように鍵生成プログラム８１で規定された関数ＡＰＩ１を基に、識別データＳＩＤ１，ＳＩＤ２，ＳＩＤ３と、原鍵データＫＯを鍵管理部３３から入力する。

ステップＳＴ１２：

鍵生成部３４は、前述したように認証プログラム８０で規定された関数ＡＰＩ２を基に、装置識別データＩＤＭを鍵管理部３３から入力する。

ステップＳＴ１３：

鍵生成部３４は、前述したように鍵保存プログラム８２で規定された関数ＡＰＩ３を基に、マスタ鍵データＫＭを鍵保存部３５から入力する。

ステップＳＴ１４：

鍵生成部３４は、ステップＳＴ１１で入力した識別データＳＩＤ２と、ステップＳＴ１２で入力した装置識別データＩＤＭと、ステップＳＴ１３で入力したマスタ鍵データＫＭとを加算してデータＸを生成する。

このように、鍵生成部３４では、ステップＳＴ１１で入力した識別データＳＩＤ１，ＳＩＤ２，ＳＩＤ３のうち識別データＳＩＤ２をデータＸの生成に用い、識別データＳＩＤ１，ＳＩＤ３をデータＸの生成に用いない。これにより、カード処理部３２および鍵管理部３３を規定する認証プログラム８０から、鍵生成プログラム８１の処理を秘密にできる。

ステップＳＴ１５：

鍵生成部３４は、ステップＳＴ１１で入力した原鍵データＫＯを、ステップＳＴ１４で生成したデータＸの値分だけ右をローテートシフトして個別鍵データＫＩを生成する。

ステップＳＴ１６：

鍵生成部３４は、ステップＳＴ１３で生成した個別鍵データＫＩを鍵管理部３３に出力する。

【００３２】

なお、鍵生成部３４が鍵データＫＩの生成に用いる個別鍵生成プログラムＫＰＲＧとして、例えば、ＩＣ１５との間の処理内容毎、例えば処理対象のファイルシステム上での位置毎、例えばエリアコード毎に異なるアルゴリズムのプログラムを用意し、指定された識別データＳＩＤ２に対応するプログラムを選択して実行してもよい。

また、鍵生成部３４は、マスタ鍵データＫＭを用いずに個別鍵データＫＩを生成してもよい。

また、個別鍵データの図７に示す生成手順は一例であり、本発明はこれに限定されるものではない。

【００３３】

このように、鍵生成部３４では、マスタ鍵データＫＭの他に、装置識別データＩＤＭと、識別データＳＩＤと、鍵データＫ（ＫＯ）とを用いて個別鍵データを生成することで、これらのデータに鍵生成に関してマスタ鍵データと同等の役割を持たせることができる。そのため、鍵管理データＫＭＤの設定に関する権限を有する事業者等が認証に用いる鍵データに関する設定を自由に変更させることができる。

また、上述したように、ファイルシステム上での位置等を基に、個別鍵生成プログラムＫＰＲＧが異なるアルゴリズムを基に個別鍵データを生成することで、よりセキュリティを高めることができる。すなわち、一部のエリア・サービス用のロジックが漏洩した場合でも、他のエリア・サービスのセキュリティを保つことができる。

【００３４】

以下、図１に示すカードシステム１の動作例を説明する。

〔第１の動作例〕

当該動作例では、ＳＡＭ１２に鍵管理データＫＭＤを設定する場合を説明する。

図１０は、当該動作例を説明するためのフローチャートである。

ステップＳＴ２１：

図１に示す管理装置１３が、図６に示すように、鍵管理データＫＭＤを設定用マスタ鍵データＫＰＭで暗号化した鍵パッケージデータＫＰを生成し、これをＳＡＭ１２に出力する。

ステップＳＴ２２：

ＳＡＭ１２は、インタフェース３１を介して入力した鍵パッケージデータＫＰを、図４に示す鍵管理部３３あるいは図示しない復号部において、設定用マスタ鍵データＫＰＭを用いて復号して鍵管理データＫＭＤを生成する。

ステップＳＴ２３：

鍵管理部３３は、ステップＳＴ２２で生成した鍵管理データＫＭＤを保持する。

【００３５】

〔第２の動作例〕

当該動作例では、図５を基にＩＣカード１０ｂのＩＣ１５と、ＳＡＭ１２との間でサービスに関する処理を行う場合の動作例を説明する。

図１１および図１２は、当該動作例を説明するためのフローチャートである。

ステップＳＴ３１：

ユーザが図１に示すＲ／Ｗ１１にＩＣカード１０を装着し、例えば、Ｒ／Ｗ１１に設けられた操作部を用いて自らが希望するサービスを指定する。なお、当該サービスの指定は、ＩＣ１５あるいはＳＡＭ１２が自動的に行ってもよい。

これにより、ＩＣ１５からＳＡＭ１２に、指定されたサービスの識別データＳＩＤと、ＩＣ１５のメモリ２２から読み出された装置識別データＩＤＭとがＳＡＭ１２に出力される。

【００３６】

ステップＳＴ３２：

カード処理部３２は、ステップＳＴ３１で入力した識別データＳＩＤを含む鍵要求ＫＲＥＱを鍵管理部３３に出力する。

ステップＳＴ３３：

鍵管理部３３は、鍵管理データＫＭＤを参照し、ステップＳＴ２２で入力した鍵要求ＫＲＥＱに含まれる識別データＳＩＤに対応付けられた鍵データＫが、個

別鍵および固定鍵の何れであるかを特定する。

ステップＳＴ３４：

鍵管理部３３は、ステップＳＴ３３で固定鍵であると特定した場合にステップＳＴ３５に進み、個別鍵であると特定した場合にステップＳＴ３８に進む。

【００３７】

ステップＳＴ３５：

鍵管理部３３は、鍵管理データＫＭＤを参照して、ステップＳＴ３２で入力した識別データＳＩＤに対応する鍵データ（固定鍵データ）を得る。

ステップＳＴ３６：

鍵管理部３３は、ステップＳＴ３５で得た鍵データ、あるいは後述するステップＳＴ４２で鍵生成部３４から入力した鍵データをカード処理部３２に出力する。

【００３８】

ステップＳＴ３７：

カード処理部３２は、ステップＳＴ３６で入力した鍵データを基に、ＩＣ１５との間で相互認証を行い、互いの正当性を確認すると、ステップＳＴ３１で入力した識別データＳＩＤに対応するサービス処理をＩＣ１５と連携して行う。

【００３９】

ステップＳＴ３８：

鍵管理部３３は、ステップＳＴ３４で個別鍵であると特定された場合に、カード処理部３２に装置識別データＩＤＭを要求する要求ＩＤＭ__ＲＥＱを出力する。

ステップＳＴ３９：

カード処理部３２は、ステップＳＴ３８で入力した要求ＩＤＭ__ＲＥＱに応じて、ステップＳＴ３１でＩＣ１５から入力した装置識別データＩＤＭを鍵管理部３３に出力する。

ステップＳＴ４０：

鍵管理部３３は、鍵管理データＫＭＤから識別データＳＩＤに対応する鍵データＫＯを読み出す。

そして、鍵管理部３３は、鍵データＫＯと、ステップＳＴ３９で入力した装置識別データＩＤＭと、ステップＳＴ３２で入力した識別データＳＩＤとを鍵生成部３４に出力する。

【００４０】

ステップＳＴ４１：

鍵生成部３４は、図７を用いて説明した手順で、ステップＳＴ３３で入力した鍵データ等を用いて、個別鍵データＫＩを生成する。

ステップＳＴ４２：

鍵生成部３４は、ステップＳＴ４１で入力した個別鍵データＫＩを鍵管理部３３に出力する。

【００４１】

以上説明したように、カードシステム１では、図６を用いて説明したように、ＳＡＭ１２において、認証プログラム８０から鍵生成プログラム８１に、識別データＳＩＤ１～ＳＩＤ３を提供し、鍵生成プログラム８１において識別データＳＩＤ２のみを用いて個別鍵データＫＩを生成する。そのため、認証プログラム８０の開発者が鍵生成プログラム８１に提供する識別データを基に鍵生成プログラム８１における鍵生成アルゴリズムを推測することを困難にできる。

【００４２】

また、ＳＡＭ１２では、図７に示すようにファイアウォールＦＷ１，ＦＷ２が規定されているため、認証プログラム８０が鍵生成プログラム８１に不正にアクセスすることを防止でき、鍵生成プログラム８１における鍵生成アルゴリズムをセキュアにできる。

【００４３】

また、ＳＡＭ１２では、認証プログラム８０と鍵生成プログラム８１とが関数ＡＰＩ１，ＡＰＩ２を介してデータ授受を行うこと以外完全に独立したプログラムであるため、認証プログラム８０と鍵生成プログラム８１との開発を異なる開発者が並行して進めることができる。

【００４４】

また、ＳＡＭ１２では、認証プログラム８０および鍵生成プログラム８１とは

独立して、鍵保存プログラム８２をＳＡＭ１２の外部からダウンロードするように構成することで、鍵生成プログラム８１に影響を与えることなく、鍵生成プログラム８１を更新できる。例えば、所定のサービスを提供する事業者が鍵生成プログラム８１を作製した場合に、鍵保存プログラム８２を更新しても、当該事業者は鍵生成プログラム８１を更新する必要がなく、負担を軽減できる。

【００４５】

また、カードシステム１では、ＳＡＭ１２は、ＩＣ１５との間でのサービス処理に先立って、ＩＣ１５から受けたＩＣカード１０（ＩＣ１５）に固有の装置識別データＩＤＭを基に、当該ＩＣ１５に固有の個別鍵データＫＩを生成し、個別鍵データＫＩを基にＩＣ１５との間で相互認証を行う。

そのため、複数のＩＣカード１０のうち一部のＩＣカード１０の個別鍵データＫＩの秘匿性が失われた場合でも、他のＩＣカード１０の個別鍵データの秘匿性は失われず、セキュリティを高めることができる。

【００４６】

また、カードシステム１によれば、サービス等を識別する識別データＳＩＤをＩＣ１５からＳＡＭ１２に出力し、ＳＡＭ１２において識別データＳＩＤを基に個別鍵生成のアルゴリズムを切り換えるため、一部のアルゴリズムの秘匿性が失われた場合での、その他のアルゴリズムを基にした個別鍵データの秘匿性を保つことができる。

【００４７】

また、カードシステム１によれば、サービス等を識別する識別データＳＩＤをＩＣ１５からＳＡＭ１２に出力し、ＳＡＭ１２において識別データＳＩＤを基に認証に用いる鍵データが個別鍵および固定鍵のいずれであるかを判断するため、ＩＣ１５では、認証に用いる鍵データが個別鍵および固定鍵のいずれであるかを意識せずに処理を行うことができる。

【００４８】

また、カードシステム１によれば、個別鍵および固定鍵に対応した処理の切り換えを鍵管理部３３が行うため、カード処理部３２は、認証に用いる鍵データが個別鍵および固定鍵のいずれであるかを特定せずに処理を行うことができる。そ

のため、カード処理部３２の開発に伴う負担を軽減できると共に、個別鍵を用いた認証に関する情報がカード処理部３２の開発者に漏れることを防止できる。

【００４９】

また、カードシステム１によれば、鍵管理データＫＭＤの鍵特定データＫＰＤにおいて、全ての鍵データについてその特性を固定鍵とすることで、固定鍵のみを用いるシステムと互換性をとることができる。

【００５０】

また、カードシステム１によれば、カード処理部３２の動作とは独立して、鍵管理部３３において鍵管理データＫＭＤを基に個別鍵データに係わる処理を行うため、個別鍵データに関する情報を、カード処理部３２のアプリケーションプログラムの開発者に知られないようにすることができる。すなわち、個別鍵データに関する情報を、鍵管理データＫＭＤ、並びに個別鍵生成プログラムＫＰＲＧの設定・開発者のみに閉じることができ、高いセキュリティを実現できる。

【００５１】

カードシステム１によれば、ＳＡＭ１２は、上述したように装置識別データＩＤＭを基に個別鍵データを生成することで、全てのＩＣカード１０の個別鍵データを記憶している必要がないため、小規模なメモリを用いて構成できる。

【００５２】

本発明は上述した実施形態には限定されない。

また、上述した実施形態では、本発明の認証先としてＩＣカード１０のＩＣ１５を例示したが、認証先はコンピュータなどであってもよい。

【００５３】

【発明の効果】

本発明によれば、鍵生成手段における鍵データの生成手法を認証手段の開発者に秘密にできるデータ処理装置およびその方法を提供することができる。

また、本発明によれば、鍵生成のアルゴリズムを認証プログラムに対して秘匿にできるプログラムを提供することができる。

【図面の簡単な説明】

【図１】

図１は、本発明の実施形態のカードシステムの構成図である。

【図２】

図２は、図１に示すＩＣカードに内蔵されたＩＣの構成図である。

【図３】

図３は、図１に示すＩＣ内に規定された各種の鍵データを説明するための図である。

【図４】

図４は、図１に示すＳＡＭの機能ブロック図である。

【図５】

図５は、図４に示すＳＡＭの処理を説明するための図である。

【図６】

図６は、図５に示すＳＡＭのソフトウェア構成を説明するための図である。

【図７】

図７は、図６に示すＳＡＭ内のプログラムに規定されたファイアウォールを説明するための図である。

【図８】

図８は、図５に示すＳＡＭへの鍵管理データの登録を説明するための図である。

【図９】

図９は、図５に示す鍵生成部における個別鍵データの生成手順を説明するためのフローチャートである。

【図１０】

図１０は、図５に示すＳＡＭへの鍵管理データの登録の手順を説明するためのフローチャートである。

【図１１】

図１１は、図５に示すＩＣカードのＩＣと、ＳＡＭとの間でサービスに関する処理を行う場合の動作例を説明するためのフローチャートである。

【図１２】

図１２は、図５に示すＩＣカードのＩＣと、ＳＡＭとの間でサービスに関する

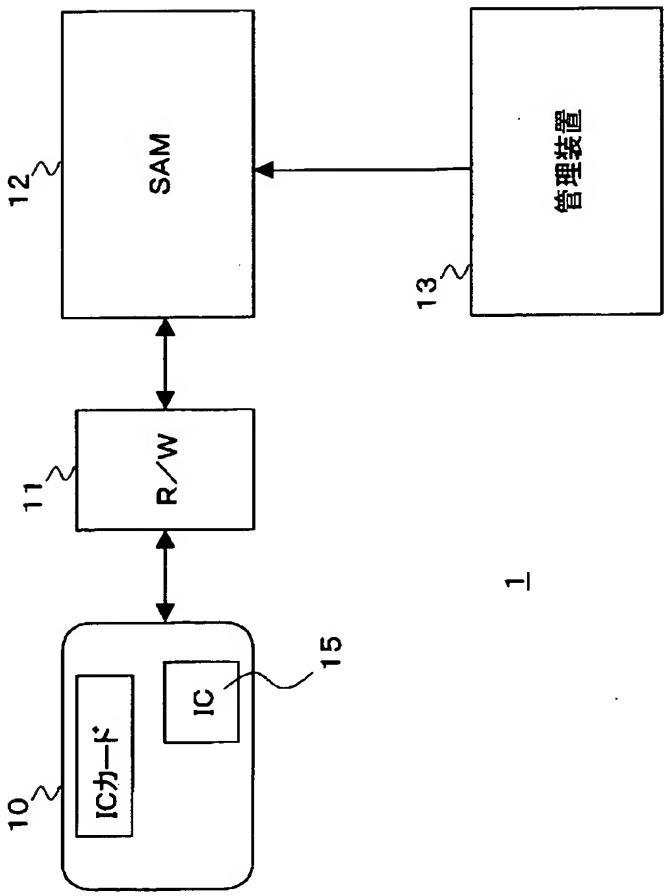
処理を行う場合の動作例を説明するための図１１の続きのフローチャートである。

【符号の説明】

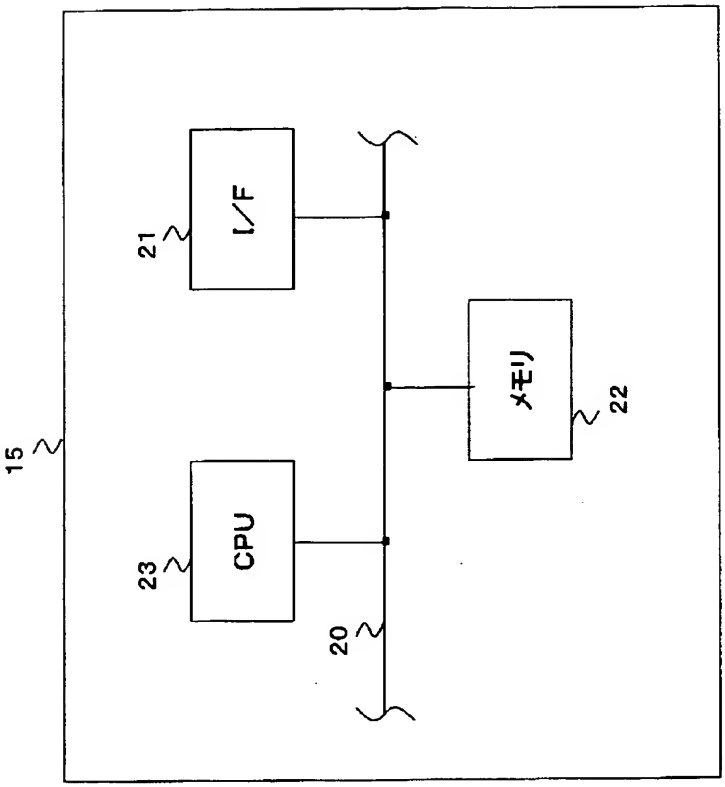
１…カードシステム、１０…ＩＣカード、１１…Ｒ／Ｗ、１２…ＳＡＭ、１３円管理装置、１５…ＩＣ、２０…内部バス、２１…インタフェース、２２…メモリ、２３…ＣＰＵ、３０…内部バス、３１…インタフェース、３２…カード処理部、３３…鍵管理部、３４…鍵生成部、３５…鍵保存部、８０…認証プログラム、８１…鍵生成プログラム、８２…鍵保存プログラム、ＦＷ１，ＦＷ２…ファイアウォール

【書類名】　図面

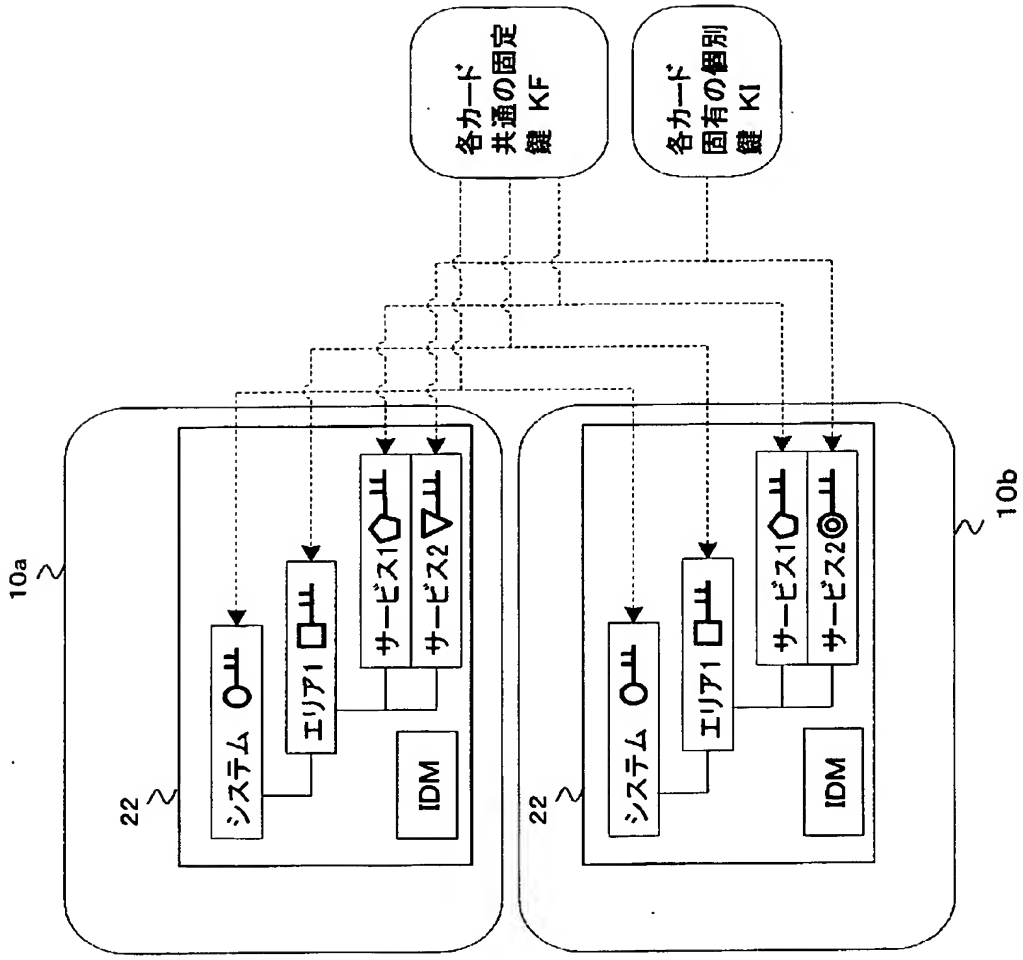
【図１】



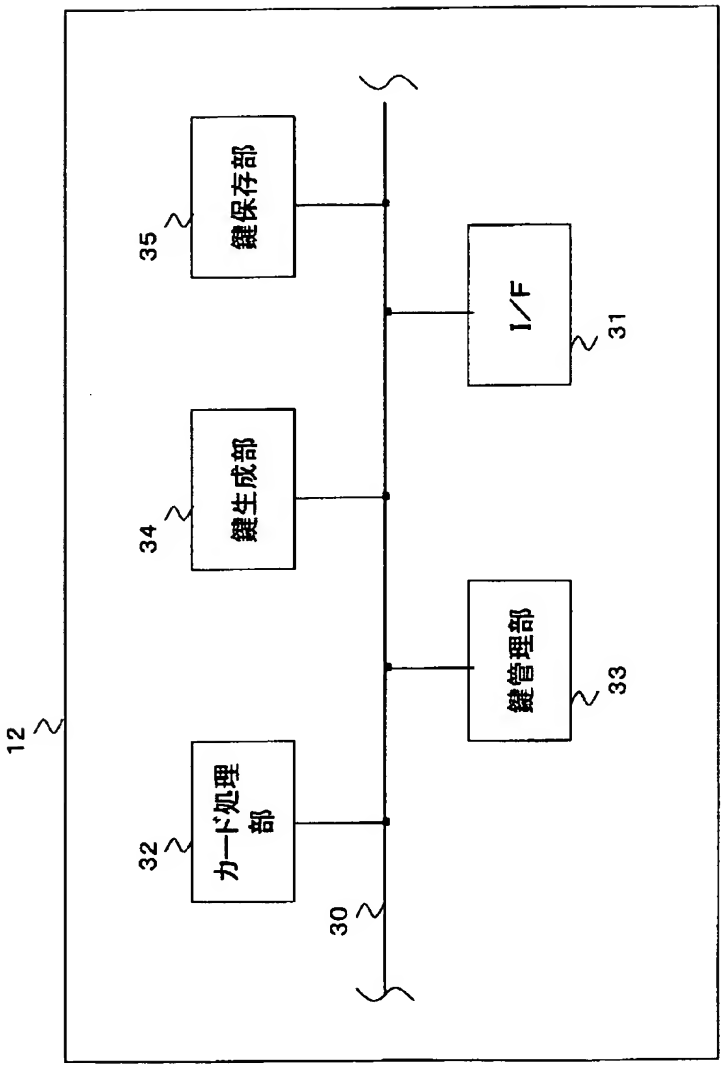
【図２】



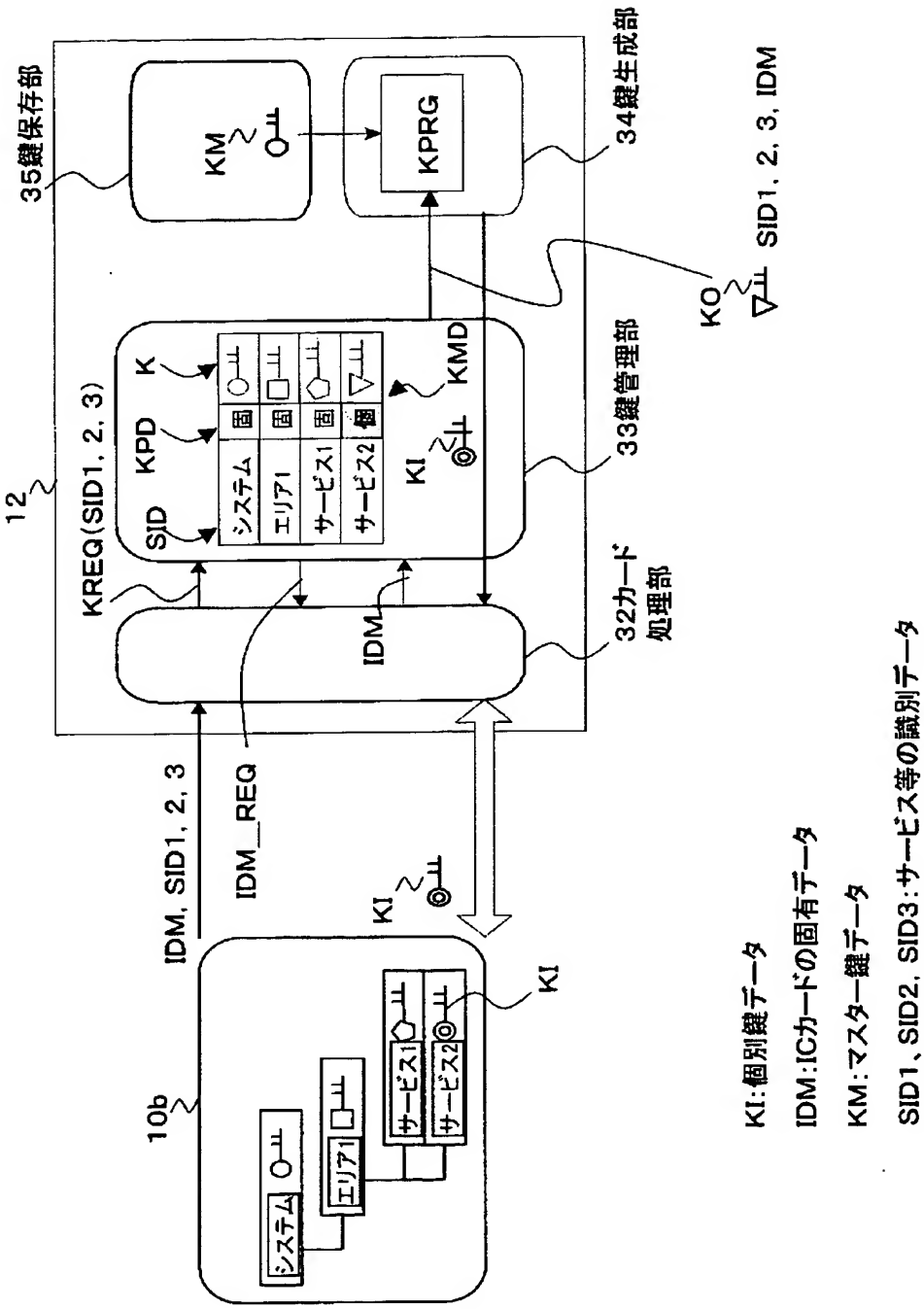
【図３】


各カード
共通の固定
鍵 KF
各カード
固有の個別
鍵 KI
10a
10b
22
22
システム
エリア1
サービス1
サービス2
IDM
システム
エリア1
サービス1
サービス2
IDM

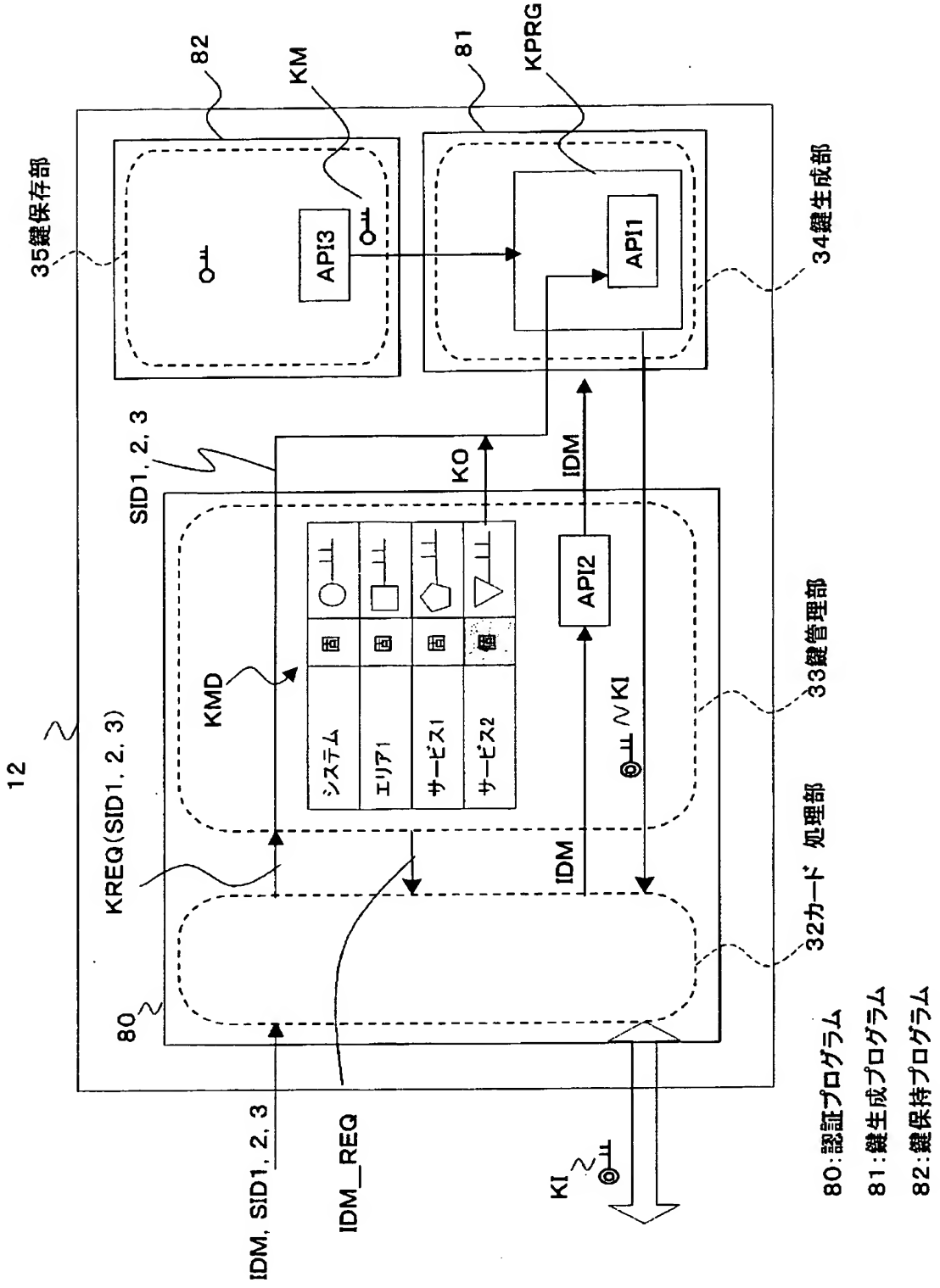
【図４】



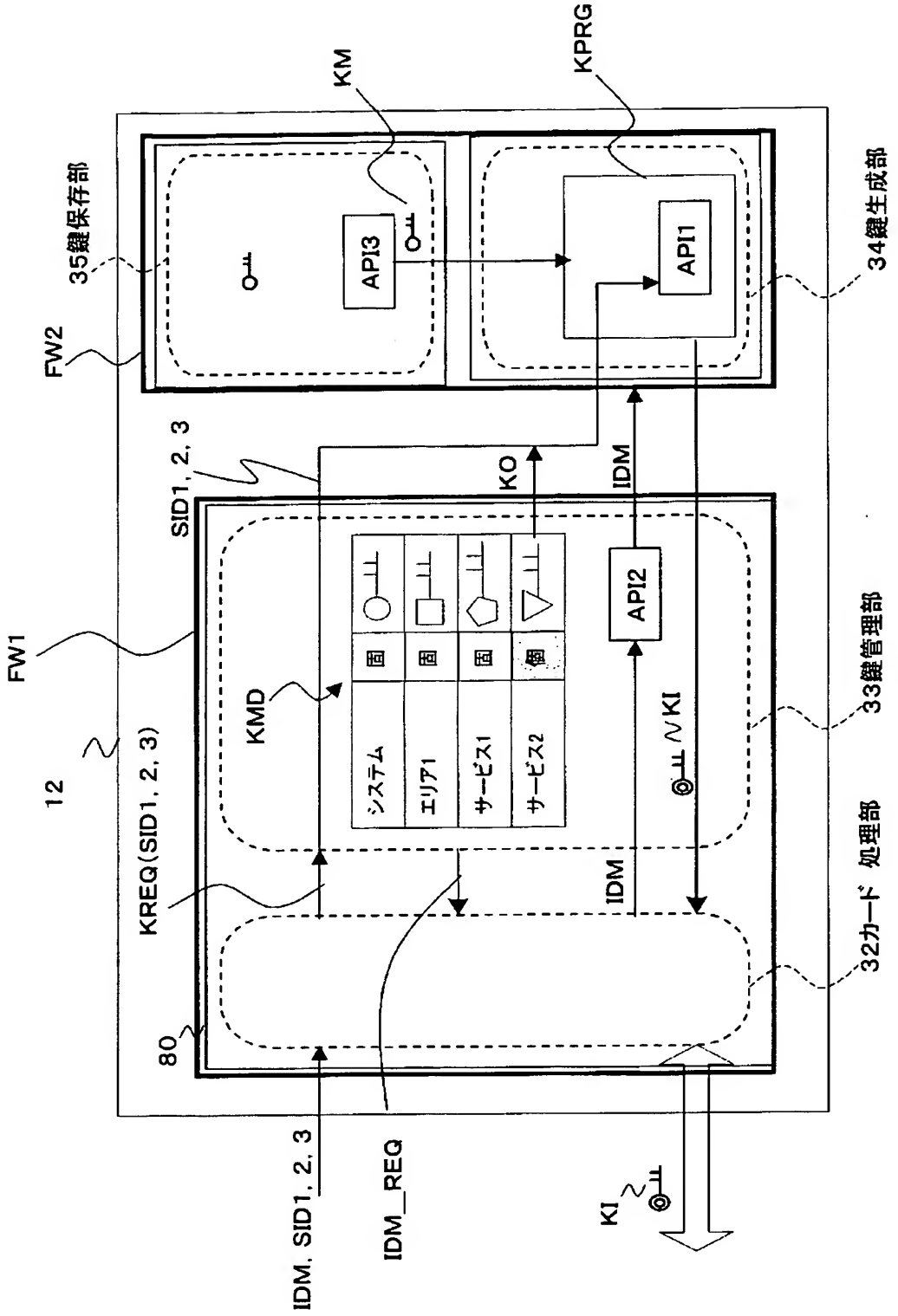
【図５】


35鍵保存部
KM
KPRG
34鍵生成部
SID1, 2, 3, IDM
KO
12
KREQ(SID1, 2, 3)
SID
KPD
K
KMD
KI
システム
エリア1
サービス1
サービス2
33鍵管理部
IDM
32カード処理部
IDM, SID1, 2, 3
IDM_REQ
KI
KI
10b
KI:個別鍵データ
IDM:ICカードの固有データ
KM:マスター鍵データ
SID1、SID2, SID3:サービス等の識別データ

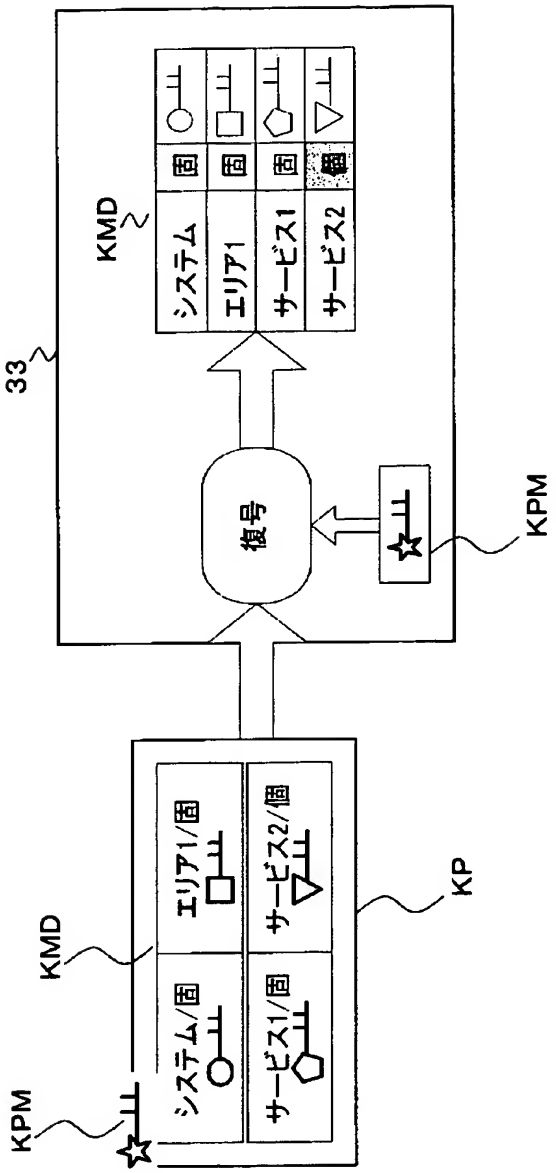
【図６】


82
KM
81
KPRG
35鍵保存部
API3
API1
34鍵生成部
SID1, 2, 3
KO
IDM
KMD
システム
エリア1
サービス1
サービス2
API2
KI
33鍵管理部
12
KREQ(SID1, 2, 3)
IDM
32カード 処理部
80
IDM, SID1, 2, 3
IDM_REQ
KI
80:認証プログラム
81:鍵生成プログラム
82:鍵保持プログラム

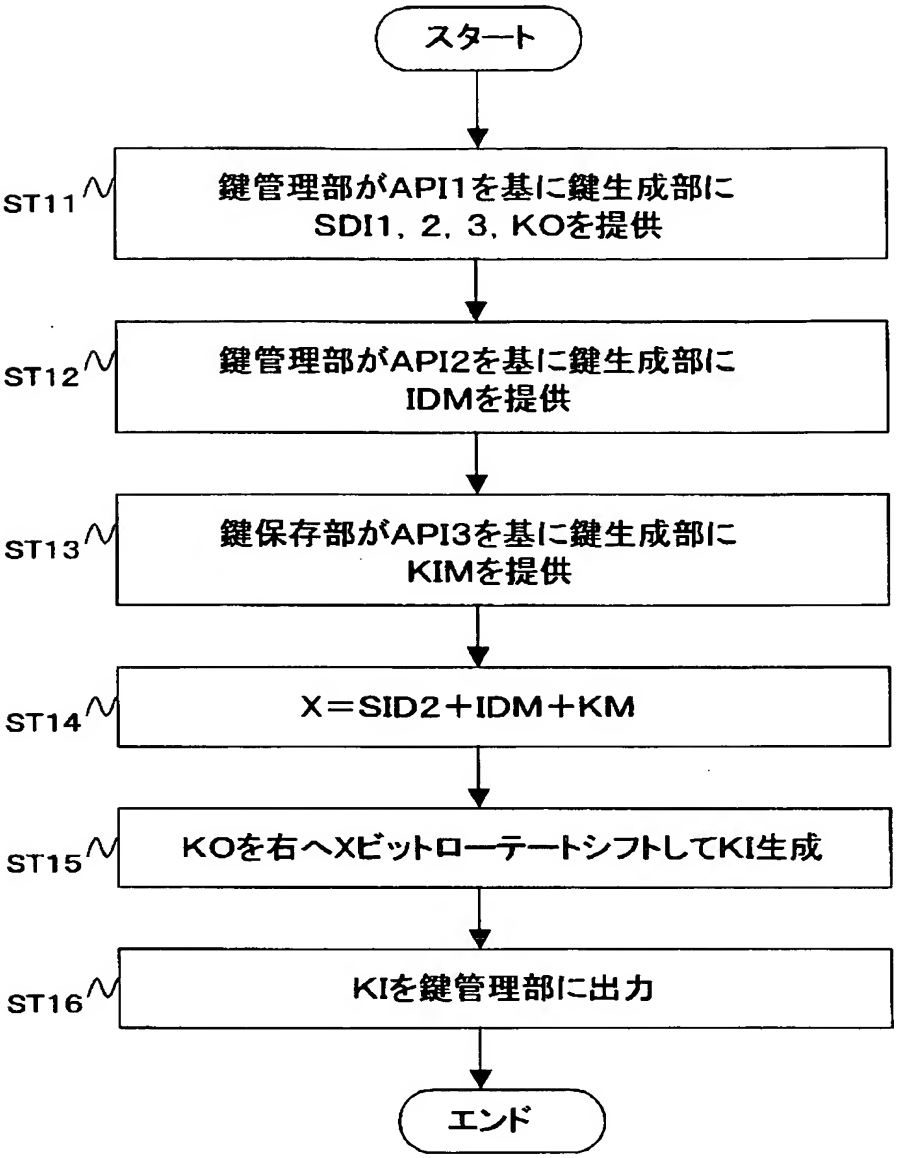
【図７】


KM
KPRG
35鍵保存部
34鍵生成部
API3
API1
FW2
SID1, 2, 3
KO
IDM
FW1
KMD
システム
エリア1
サービス1
サービス2
固
個
API2
KI
33鍵管理部
12
KREQ(SID1, 2, 3)
32カード処理部
80
IDM
IDM, SID1, 2, 3
IDM_REQ
KI

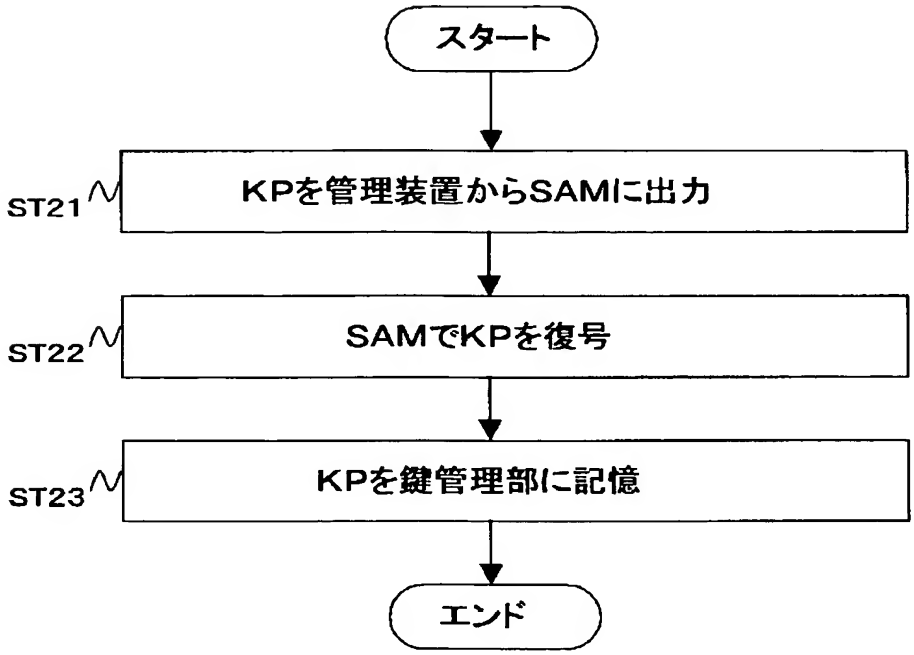
【図８】


KMD
33
システム
エリア1
サービス1
サービス2
面
面
面
面
復号
KPM
KMD
KP
KPM
システム/面
エリア1/面
サービス1/面
サービス2/個
KMD:鍵管理データ
KP:鍵パッケージ

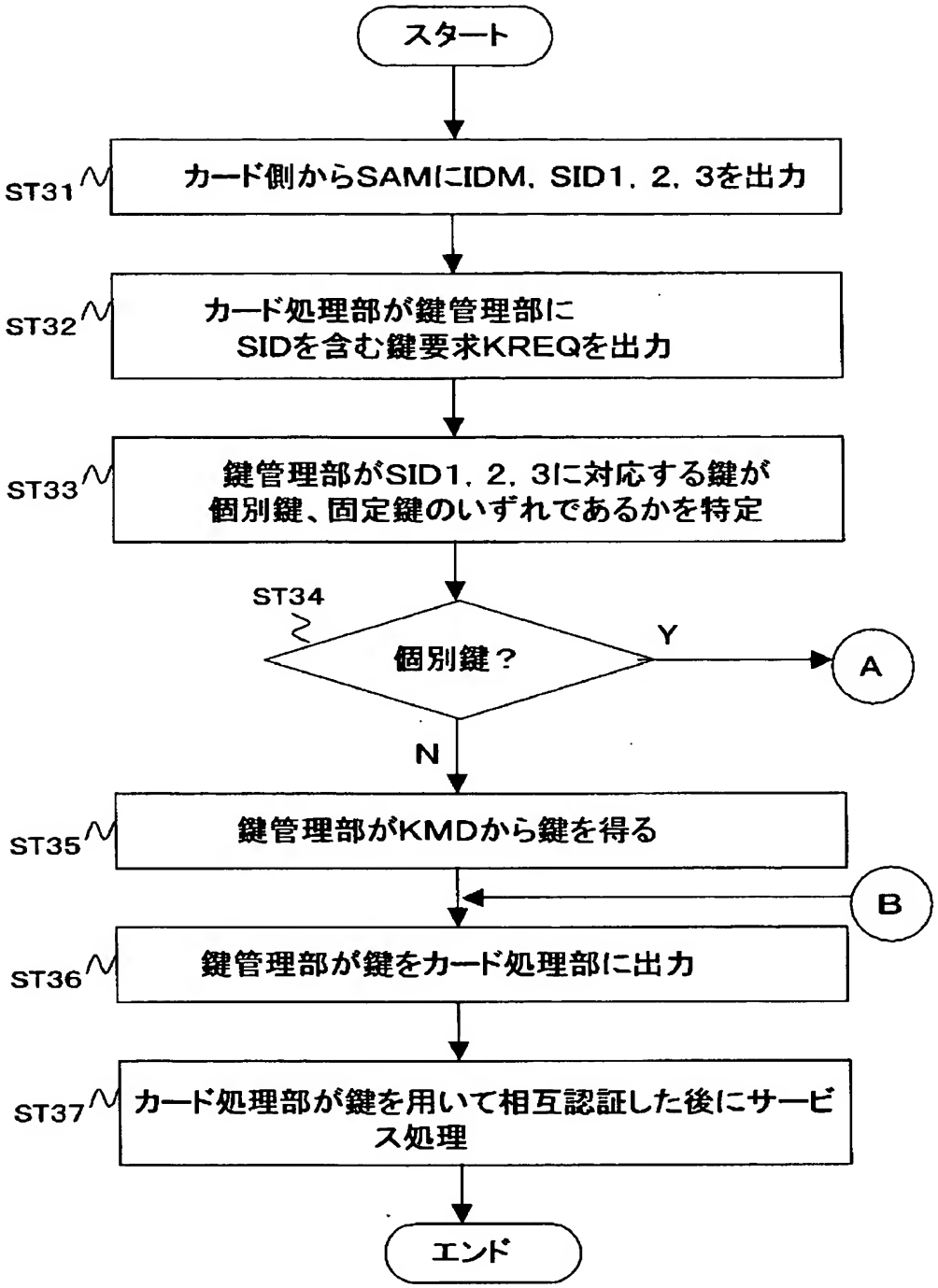
【図９】


スタート
ST11
鍵管理部がAPI1を基に鍵生成部に
SDI1，2，3，KOを提供
ST12
鍵管理部がAPI2を基に鍵生成部に
IDMを提供
ST13
鍵保存部がAPI3を基に鍵生成部に
KIMを提供
ST14
X＝SID2＋IDM＋KM
ST15
KOを右へXビットローテートシフトしてKI生成
ST16
KIを鍵管理部に出力
エンド

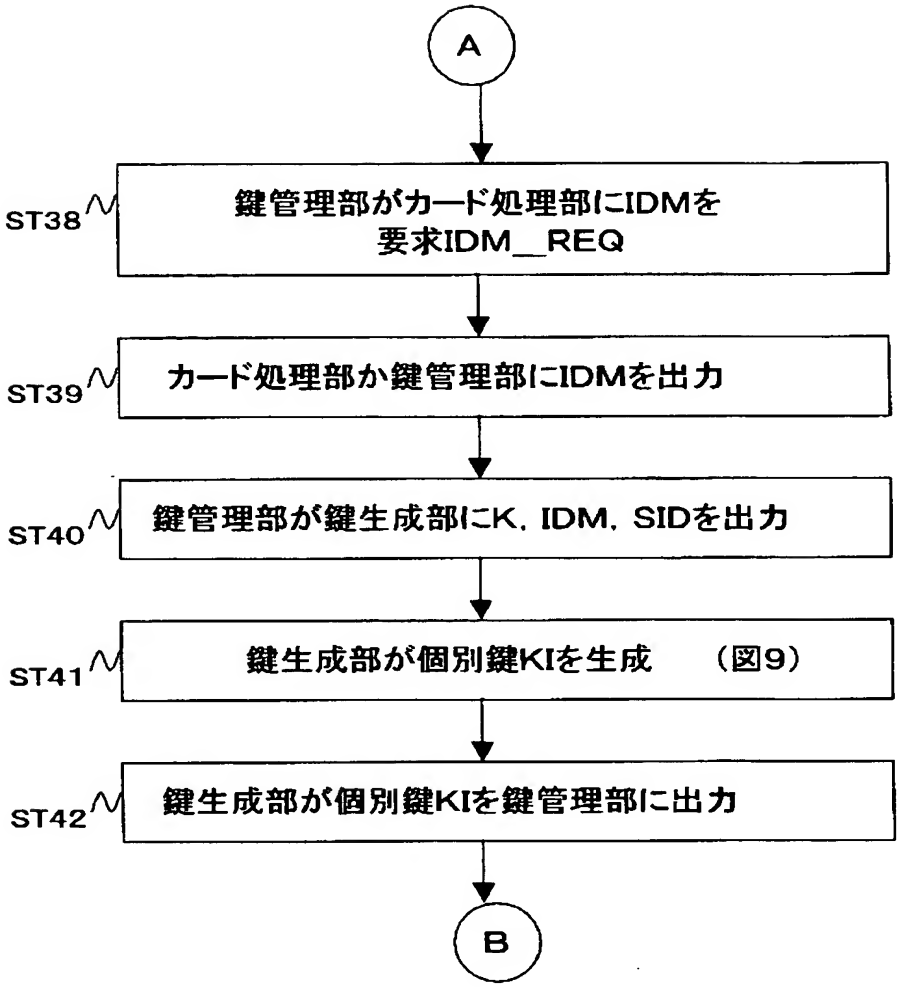
【図１０】


スタート
ST21
KPを管理装置からSAMに出力
ST22
SAMでKPを復号
ST23
KPを鍵管理部に記憶
エンド

【図１１】


スタート
ST31
カード側からSAMにIDM、SID1，2，3を出力
ST32
カード処理部が鍵管理部に
SIDを含む鍵要求KREQを出力
ST33
鍵管理部がSID1，2，3に対応する鍵が
個別鍵、固定鍵のいずれであるかを特定
ST34
個別鍵？
Y
A
N
ST35
鍵管理部がKMDから鍵を得る
B
ST36
鍵管理部が鍵をカード処理部に出力
ST37
カード処理部が鍵を用いて相互認証した後にサービス処理
エンド

【図１２】


A
ST38
鍵管理部がカード処理部にIDMを要求IDM__REQ
ST39
カード処理部か鍵管理部にIDMを出力
ST40
鍵管理部が鍵生成部にK，IDM，SIDを出力
ST41
鍵生成部が個別鍵KIを生成　（図9）
ST42
鍵生成部が個別鍵KIを鍵管理部に出力
B

【書類名】　要約書

【要約】

【課題】　鍵生成手段における鍵データの生成手法を認証手段の開発者に秘密にできるデータ処理装置を提供する。

【解決手段】　認証プログラム８０は、鍵生成プログラム８１内の関数ＡＰＩ１を呼び出し、当該関数ＡＰＩ１の入力パラメータとして、ＩＣカードのＩＣ５から入力したサービス等の識別データＳＩＤ１，２，３を代入する記述を有する。認証プログラム８０を基にした当該コードの実行に応じて、所定のアドレスに書き込まれた識別データＳＩＤ１，２，３を入力パラメータとして用いて鍵生成プログラム８１が鍵生成を行う。

【選択図】　図６

特願２００３－０７０３０１

出　願　人　履　歴　情　報

識別番号　　［０００００２１８５］

１．変更年月日　　１９９０年　８月３０日
［変更理由］　　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社